REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Fall 1998	Newsletter Vol. 2 No. 2

4. TITLE AND SUBTITLE
Information Assurance Technology
IA Newsletter

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Assurance Technology Analysis Center

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

A

13. ABSTRACT ***(Maximum 200 Words)***

The IANewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). This issue continues the foucs on current information assurance initiatives underway within DoD, academia, and industry. In addition, an overview of the current collection of Firewall Tools is provided. Also, featured in the issue:
Protecting Our Critical Infrastructures Through Public-Private Partnership
Detecting Intrusions Cooperatively Across Multiple Domains
Secure Your Distributed Network: What Will It Take?

14. SUBJECT TERMS
Information Security, Information Assurance, Information Operations, Intrusion Detection

15. NUMBER OF PAGES
16

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None

INFORMATION ASSURANCE TECHNOLOGY

IA newsletter

Vol. 2, No. 2
Fall 1998

The Defense-Wide Information Assurance Program

by CAPT J. Katharine Burton, USN
DIAP, OASD (C3I)/IA

The Department of Defense's increasing dependence on a global information environment heightens its exposure and vulnerability to a rapidly growing number of sophisticated internal and external threats. Globally inter-networked and interdependent information systems tend to *level the playing field* between allies and potential adversaries. These systems offer adversaries access to potentially low-risk, high-value information infrastructure targets with the potential to impact the full spectrum of DoD operations. Furthermore, with each advance in information technology, new vulnerabilities are created that must be quickly discovered and effectively neutralized.

Before global networking became commonplace, the majority of the Department's critical information functions, both command & control and support, were electrically separated in Component-managed telecommunications and information processing environments. This separate-system condition had the advantage of providing the Department's information and information systems a level of resiliency and protection, forcing an adversary to attack each independently controlled environment. To seriously degrade the aggregate capability of the Department, an adversary must disrupt or corrupt a large number of critical systems using highly sophisticated (and largely unavailable) technologies that were expensive in terms of both time and money.

In contrast, the Department's reliance on commercial, globally interconnected information technologies has markedly heightened its vulnerability to attack. Today's inter-networked information technologies make it possible to affect many users, systems, and networks by attacking a single connection to a single network. To attack a large number of systems, an adversary need only find and attack a single exploitable connection to the system. These attacks can be performed through the use of a large and growing variety of available and inexpensive hacker tools. Once inside a system, an adversary can exploit it, as well as the systems networked to it. This glob-

continued on page 2

Internet Presents WEB of SECURITY ISSUES

by Paul Stone
American Forces Information Service

milies—sim-
cruising the
t.
n and Ash-
ley, mem-
bers of the
Pentagon's
ıff, were not
ı a joke on
eaders. Nor
ıey trying to
be clever. Rather they were dramatically, and effectively demonstrating the ease of accessing and gathering personal and military data on the information highway — information which, in the wrong hands, could translate into a vulnerability.

year, Air Force Lt. Col. Buzz Walsh and Maj. Brad Ashley presented a series of briefings to top DoD leaders that raised more than just a few eyebrows.

Selected leaders were shown how it was possible to obtain their individual social security numbers, unlisted home phone numbers, and a host of other personal information about themselves

"You don't need a Ph.D. to do this," Walsh said about the ability to gather the information. "There's no rocket science in this capability. What's amazing is the ease and speed and the minimal know-how needed. The tools (of the Net) are designed for you to do this."

The concern over personal information on key DoD leaders began with a simple inquiry from one particular flag officer who said he was receiving a large number of unsolicited calls at home. In addition to having the general's unlisted number, the callers knew specifically who he was.

Too Much About Too Much

Beginning with that one inquiry, the Joint Staff set out to discover just how easy it is to collect data not only on military person-

continued on page 4

IATAC is a DoD-Sponsored Information Analysis Center Administered by the Defense Technical Information Center (DTIC).

INSIDE

continued from cover

Vol. 2 No. 2

The IANewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). This issue continues the focus on current information assurance initiatives underway within DoD, academia, and industry. In addition, an overview of the current collection of Firewall Tools is provided.

IATAC, a DoD-Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about IATAC capabilities, products and services may be addressed to:

Robert Thompson
Director, IATAC
703.902.5530

We welcome your input!
To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:

IATAC
ATTN: C. McNemar
8283 Greensboro Dr.
McLean, VA 22102
Phone 703.902.3177
Fax 703.902.3425
STU-III 703.902.5869
STU-III Fax 902.3991

E-mail: iatac@dtic.mil
URL: www.iatac.dtic.mil

Art & Production Director
C. McNemar
Information Processing
Robert Weinhold
Information Collection
Alethia A. Tucker
Inquiry Services
Peggy O'Connor
Contributing Editor
Martha Elim

al marriage of systems and networks has created *a shared risk environment.*

Any risk of weakness in any portion of the Defense Information Infrastructure (DII) is a serious threat to the operational readiness of all Components. The Department is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information, and the protection of its infrastructure. Recent assessments, exercises, and real-life events clearly demonstrate that Defense-wide improvements in Information Assurance (IA) are an absolute and continuous operational necessity. We can no longer be satisfied with reactive or after-the-fact solutions. As the Department modernizes its information infrastructure, it must continuously invest in the research, development, and timely integration of products, procedures, and training necessary to sustain its ability to defend and protect the infrastructure. Providing for the protection of the DII is among the Department's highest priorities and is one of its most formidable challenges.

The Department's IA objective is to provide for the availability, integrity, authentication, confidentiality, non-repudiation, and rapid restoration of DII mission essential elements. Critical to achieving this objective is the implementation of a Department-wide planning and integration framework. To that end, on January 30 the Deputy Secretary of Defense, Dr. John J. Hamre, approved the creation of the Defense-wide Information Assurance Program (DIAP). The recommendations of the program are the result of several years of effort by the IA community, including:

- The October 9, 1996, Program Decision Memorandum II (PDM II) directing that an assessment be conducted by the Department-wide Information Assurance Task Force, and
- The August-September 1997 IA Integrated Process Team (IA IPT) effort directed by a Secretary of Defense memorandum of August 12, 1997.

The recommendations reflect the Department's understanding that IA is an operational readiness issue and that its dependence on inter-networked systems and services creates a shared risk environment necessitating an unprecedented level of coordination and unity across the Department. The DIAP will provide the common management framework and central oversight necessary to ensure the protection and reliability of the DII. While planning and integration will be centralized, execution of individual Components' programs will remain the responsibility of the Components. A culture that recognizes and values IA must also be built among all Department Components.

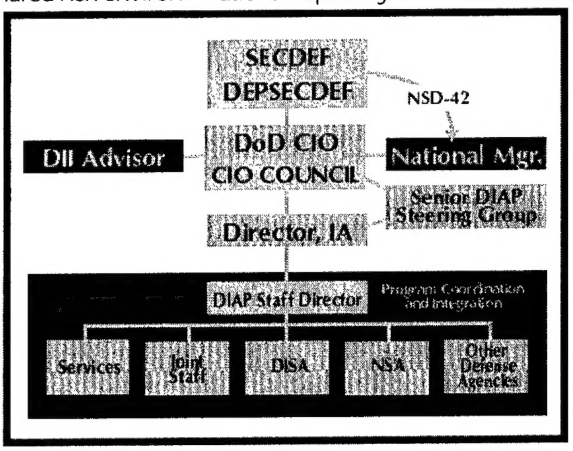


Figure 1.

Accordingly, the DIAP will continuously compare Department's IA programs and functions against its operational and business information requirements, Defense-wide readiness standards, and threats to the DII. The DIAP will also infuse IA throughout its operations as a fundamental element of readiness and training. Operational readiness standards will be used to assess the adequacy of the protection afforded to the Department's data, information systems, and networks, and to the entire DII. This effort will provide a comprehensive and real-time picture of all IA programs. It will enable the Department to accurately develop, validate, and prioritize IA requirements; determine the return on its IA investments; and objectively assess its protection efforts.

The DIAP achieved initial operational capability in June 1998 with the assignment of the Staff Director and other key positions. It is in the process of achieving full operational capability as staffing for the various positions becomes available. Organizationally, the DIAP reports to the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for C3I (OASD/C3I) (Figure 1). The DIAP is divided into two teams: the Functional Evaluation and Integration Team (FEIT) and the Program Development and Integration Team (PDIT) (see Figure 2). Between

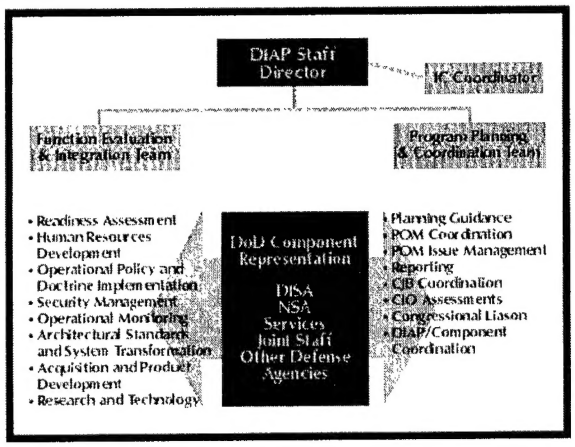


Figure 2.

Protecting Our Critical Infrastructures Through Public-Private Partnership

by Kenneth M. Geide, National Infrastructure Protection Center, FBI

As our society speeds into the Information Age, we are growing increasingly dependent on a complex web of information systems to manage our lives. We use computers, the Internet, and other information technologies to conduct business, manage finances, engage in personal communications, and process vast amounts of data.

This dependence on information systems also extends to our Nation's critical infrastructures. These infrastructures (telecommunications, energy, banking and finance, transportation, and government operations, among others) are the foundation of our economy, national security, and way of life; virtually every citizen depends on them everyday. Technological advances have made these infrastructures highly automated and interdependent, increasing their efficiency and improving the quality of their services.

Yet technological advances have also introduced vulnerabilities into these infrastructures, and more people now have the tools to exploit them. For example, the pervasiveness and easy accessibility of the Internet means that anyone possessing the right tools and technical skills can penetrate an organization's information and control systems to steal data or inflict damage. Culprits who might commit such acts include disgruntled employees, recreational hackers, criminal groups, terrorist organizations, foreign intelligence services, or even hostile nations.

The National Infrastructure Protection Center (NIPC) was established in February 1998 to address infrastructure threats and vulnerabilities. Our mission is to detect, deter, assess, warn of, respond to, and investigate unlawful acts (both physical and cyber) that threaten our critical infrastructures. Located at FBI Headquarters in Washington, D.C., the NIPC is an interagency, public-private body that brings together investigators, analysts, computer scientists, and other experts from government and private industry.

The NIPC focuses on preventing attacks (learning about them before they occur) and taking steps to prevent or disrupt them. This effort requires collecting and analyzing information from all available sources (including law enforcement, intelligence services, open sources, and the private sector) and disseminating our analyses to all relevant organizations. If an attack occurs, the NIPC is the Federal Government's focal point for crisis response and investigation.

The NIPC is built on a foundation of partnership. When fully staffed, the NIPC will include representatives from the Federal Government (including the FBI, Department of Defense, the Intelligence Community, and others), from the owners and operators of critical infrastructures (to provide expertise and to facilitate coordination in the event of a crisis), and from state and local law enforcement (to build liaison relationships with emergency first responders). The NIPC also will establish electronic connectivity to relevant organizations in government and industry that have or require information about infrastructure threats and vulnerabilities.

The NIPC's success depends on information sharing. We are developing two-way channels of communication to facilitate information flow regarding threats, vulnerabilities, and incidents between government and industry. The Federal Government has access to intelligence and law enforcement information that is unavailable to private organizations. Simultaneously, the NIPC wants to learn about the threats and vulnerabilities experienced by these organizations. Sharing this important information will help us to define the threat environment with greater accuracy, thereby enabling us to prevent or disrupt potential attacks.

One current initiative is "InfraGard," a pilot project sponsored by the FBI's Cleveland Field Office to foster information sharing among private industry, the FBI, and other government agencies. A secure, Internet-based system, InfraGard has an alert network that members can use to report computer intrusions to the FBI. Reports are sent by encrypted electronic mail (e-mail) in two forms: a detailed description (which the FBI uses for analysis and, if required, investigative purposes) and a sanitized, victim-produced version (for distribution to other InfraGard members). Approximately 56 organizations are now involved in the InfraGard project, and we are exploring options for expanding it into a national system.

Protecting our critical infrastructures in the Information Age will require creative solutions and new ways of thinking. Establishing the NIPC and developing a productive partnership between government and industry are important steps in this direction. Much work remains to be done, but we look forward to working with our partners as we confront the challenges ahead.

Kenneth Geide is Chief of the FBI's Computer Investigations and Operations Section (CIOS), National Infrastructure Protection Center (NIPC). Mr. Geide initiated the FBI's Economic Counterintelligence program and was instrumental in drafting and achieving the passage of the Economic Espionage Act of 1996. He received his Bachelor's Degree from the University of San Francisco and his Master's Degree from New York University.

continued from cover

nel, but the military in general. They used personal computers at home, used no privileged information - not even a DoD phone book - and did not use any on-line services that perform investigative searches for a fee.

In less than five minutes on the Net, Ashley, starting with only the general's name, was able to extract his complete address, unlisted phone number, and using a map search engine, build a map and driving directions to his house.

Using the same techniques and Internet search engines, they visited various military and military-related web sites to see how much and the types of data they could gather. What they discovered was too much about too much, and seemingly too little concern about the free flow of information versus what the public needs to know.

For example, one web site for a European-based installation provided more than enough information for a potential adversary to learn about its mission and to possibly craft an attack. Indeed, the web site contained an aerial photograph of the buildings in which the communication capabilities and equipment were housed. By pointing and clicking on any of the buildings, a web surfer would learn the name of the communications system housed in the building and its purpose.

"DATAMINING" MADE EASY

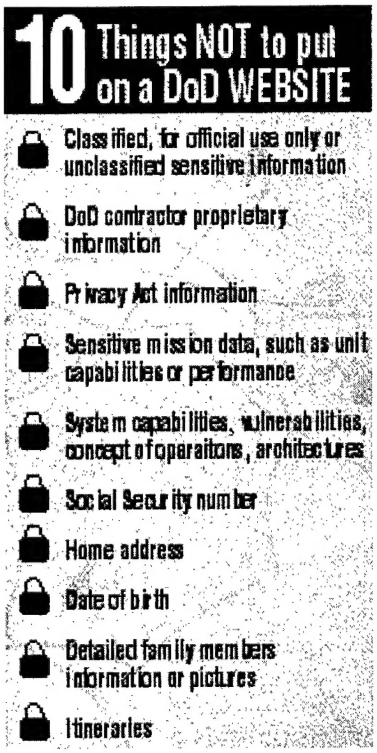
Taking their quest for easily accessible information one step further, the Joint Staff decided to see how much information could be collected just by typing a military system acronym into an Internet search engine. While not everyone would be familiar with defense-related acronyms, many of them are now batted around the airwaves on talk shows and on the Internet in military-related chat rooms. They soon discovered how easy it was to obtain information on almost any topic, with one web site hyper-linking them to another on the same topic.

What the Joint Staff was doing when they collected their information is commonly called "data mining" — surfing the Net to collect bits of information on individuals, specific topics or organizations, and then trying to piece together a complete picture. Individuals do it, organizations do it and some companies do it for profit.

While the information they discovered presented legitimate concerns, it wasn't all negative. The Army's Ft. Belvoir, Va., home page was cited as one example of a web site which served the needs of both the military and the public. It had the sort of information families or interested members of the public need and should get.

So what does all this mean? Is DoD creating individual and institutional security problems? In the rush to make information available to the internal audience, is too much being made available to the public and those who might want to inflict harm?

The Joint Staff doesn't pretend to have all the answers to these questions, but is encouraging users to think about these issues whenever they put information on the Internet; and they believe that, in some cases, DoD is it's own worst enemy.



Need To Know vs Right Too Know

Michael J. White, DoD's assistant director for security countermeasures, agrees with the Joint Staff analysis. Moreover, as a security expert, he is concerned DoD does indeed exceed what needs to be on the Internet.

"For fear of not telling our story well enough, we have told too much," he said. "Personally, I think there's too much out there...and you need to stop and ask the question: Does this next paragraph really need to be there, or can I extract enough or abstract enough so that the intent is there without the specificity? And that is hard to do because we are pressed every day. So sometimes expediency gets ahead of pausing for a minute and thinking through the process: Does the data really need to be there? Is it going to hurt me tomorrow morning?

DoD's policy on releasing information to the public, as spelled out by Defense Secretary William Cohen in April 1997, requires DoD "to make available timely and accurate information so that the public, Congress and the news media may assess and understand the facts about national security and defense strategy." The same statement requires that "information be withheld only when disclosure would adversely affect national security or threaten the men and women of the Armed Forces."

"On the one hand," Ashley said, "we have fast, cheap and easy global communication and coordination. On the other hand, we find ourselves protecting official information and essential elements of information against point-and-click aggregation. Clearly, this balancing act is a function of risk management. Full openness and full protection are equally bad answers. We have a serious education, training and awareness issue that needs to be addressed."

The Joint Staff repeatedly returns to the issue of "point-and-click aggregation" as a problem that is often overlooked when military personnel and organizations place data on the Internet. What they're referring to is the ability to collect bits of information from several different web sites to compile a more complete picture of an individual, issue or organization with very little effort.

"The biggest mistake people make is they don't understand how easy it is to aggregate information," Walsh said.

The lesson from this is that even though what is posted on the Net is perfectly innocent in and by itself, when combined with other existing information, a larger and more complete picture might be put together that was neither intended nor desired.

A more obvious problem, yet still one not always considered when posting information on the Internet, is that the "www" in web site addresses stands for "world wide" web. Information posted may be intended only for an internal audience - perhaps even a very small and very specific group of people. But on the Net, it's available to the world.

This, security experts agree, is an enormous change from the time when foreign intelligence gathering was extremely labor intensive and could only be done effectively on U.S. soil.

"If I'm a bad guy, I can sit back in the security of my homeland and spend years looking for a vulnerability before I decide to take a risk and commit resources," Ashley said. "I'm at absolutely no risk by doing that. I can pick out the most lucrative targets before hand, and may even just bookmark those targets for future use. We won't know something has been compromised until it's too late."

White agrees with the Joint Staff's concern. "You can sit in Germany and have access to the United States just as easily as you can in Australia or the People's Republic of China or Chile," White said. "It doesn't matter where you are. You can go back and forth and in between and lose your identity on the net instantaneously. Those who seek to use the system feel comfortable they won't be discovered."

FOUO Means FOUO

In addition to these issues, security experts see another recurring and disturbing problem. In the rush to take advantage of the Net's timeliness and distribution capabilities, military personnel are forgetting about or ignoring the For Official Use Only policies which previously made the information more difficult to obtain. Yet anyone using the Internet doesn't have to venture far into the array of military web sites to come across one which states: "For Official Use Only."

"We have a serious education, training and awareness issue that needs to be addressed."

If the information is For Official Use Only, security experts said web site developers, managers and commanders must ask themselves whether the information should be there in the first place.

While officials are most concerned about the information being placed on military web sites, they had similar warnings about individual or family web sites. The Joint Staff recommends the same precautions should apply at home, especially as personnel move into high-ranking, key leadership positions.

IT'S A COMMANDER'S ISSUE

At a time when the flow of information is beyond anyone's capability to either digest it or control its direction, it's not likely the problems brought forward recently by the Joint Staff will be solved any time soon. The first step, security experts said, is awareness the problems exist. Commanders have to understand not just the information capabilities of the world wide web, but the information vulnerabilities as well.

The second step, Walsh pointed out, is for commanders to become actively involved in the issue of what's being put on the Internet. Current DoD policies require that local commander, public affairs and security reviews prior to release of data on web pages. But the flow of information is so great, these reviews may not be occurring and few are looking at the aggregation problem.

"I think it would be very appropriate for a public affairs officer to be the commander's lead representative," Walsh said. "But it's a commander's issue and it should go down command lines. This is certainly an operational security issue. Just like operational security is everybody's business, this ultimately is everyone's responsibility."

White concurred and recommends installations create "security-integrated product teams" which would be tasked to develop and implement guidelines for creating and monitoring web sites on the installation.

"I think having a group come together before the (web site development) process begins will remove an awful lot of pain in the long run," White said. "We need to step back one step and think before we begin any effort, because once it's done you can't undo it. That makes it very hard in a digital environment."

Although it's not possible to retrieve what's already on the worldwide web, nor predict how it will influence future security issues, Walsh, Ashley and White believe it's not too late to make a difference. With a little more forethought and a lot more planning, it will be possible to better protect the next generation of warfighters, both on and off the battlefield, they said.

Previously released September 25, 1998 via DefenseLink, from the American Forces Information Service News Articles. Downloadable version is available at http://websecurity.afis.osd.mil.

Intrusion Detection System Evaluation

by Dr. Marc A. Zissman & Dr. Richard P. Lippmann, Lincoln Laboratory, MIT

The Information Systems Technology Group of MIT Lincoln Laboratory, under Defense Advanced Research Projects Agency Information Technology Office (DARPA/ITO) and Air Force Research Laboratory (AFRL/SNHS) sponsorship, is collecting and distributing the first standard corpus for evaluating computer network intrusion detection systems. Along with AFRL/SNHS, we are also coordinating the first formal, repeatable, and statistically significant evaluation of intrusion detection systems. This evaluation will measure probability of detection and probability of false alarm for each system under test.

This evaluation will contribute significantly to the intrusion detection research field by providing direction for research efforts by objectively calibrating current technology. The evaluation is designed to be simple, to focus on core technology issues, and to encourage wide participation. We have tried to eliminate security and privacy concerns, and we are providing data types that are used commonly by the majority of intrusion detection systems.

Technical Objective

The evaluation objectively measures intrusion detection systems' ability to detect attacks on computer systems and networks. The evaluation focuses on UNIX workstations, and the goal is to determine whether any of the following attack events occurred or were attempted during a given network session:

- Denial of service;
- Unauthorized access from a remote machine;
- Unauthorized access to local superuser privileges by a local unprivileged user;
- Surveillance and probing; and
- Anomalous user behavior.

Network sessions used for scoring the evaluation are complete TCP/IP connections, which correspond to interactions using many services including telnet, HTTP, SMTP, FTP, finger, rlogin, and others. Because the evaluation is based on the context of normal computer use on a military base, the frequency and character of the network sessions generated for each of these services reflect their actual usage at Air Force bases worldwide. The evaluation is designed to foster research progress, with the following four goals:

1. Explore promising new ideas in intrusion detection;
2. Develop advanced technology incorporating these ideas;
3. Measure the performance of this technology; and
4. Compare the performance of various newly developed and existing systems in a systematic, careful way.

Previous evaluations of intrusion detection systems have tended to focus exclusively on the probability of detection, without regard to probability of false alarm. By embedding attack sessions within normal background traffic sessions, the current evaluation will allow us to measure both detection and false alarm rates simultaneously.

Data and Guidelines

Before the evaluation begins, seven weeks of training data will be made available to the participants.

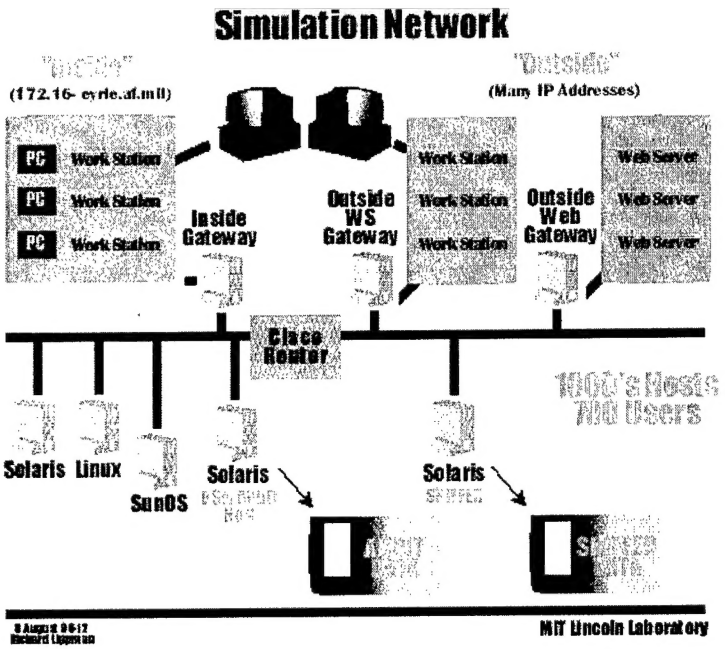


Figure 1. The Lincoln simulation network is used to generate traffic for the DARPA 1998 evaluation. The network has an "inside," which represents a military base, and an "outside," which represents the internet. Though the network contains only 10 computers, it is capable of producing traffic from thousands of simulated computers and hundreds of simulated users.

These data will be used to configure intrusion detection systems and train free parameters. Generally, the types of training data provided will be those that are used by most current commercial and research intrusion detection systems, e.g., network packet traffic, host audit files, and file system dumps. These data will be labeled individually as either normal or attack/anomalous. Later, a set of test data will be made available. Evaluation participants will run their systems blindly over the test data and will submit the system hypotheses for scoring.

Both the training and the testing data will be extracted from a simu-

lation network of about a dozen workstations (see Figure 1 on opposite page). With kernel modifications made available by AFRL/SNHS and other custom software, these few workstations can emulate thousands of workstations with hundreds of users. Both normal use and attack sessions will be present. Distributions of normal session types and normal session content will be similar to that on military bases. Attack sessions will contain old, recent, and new attacks. Most network sessions are run automatically, while a small number of sessions are generated by live users. Seven weeks of network traffic are available for training, and another two weeks will be used for evaluation. In all, the evaluation corpus will contain millions of network connections.

There are two parts to the intrusion detection evaluation. The first part is an off-line evaluation. Network traffic and audit logs collected on a simulation network will serve as input to intrusion detection systems under test. These systems will process data in batch mode, trying to find the attack sessions in the midst of normal activity. The second part of the evaluation is conducted in real-time. Systems will be delivered to AFRL/SNHS and inserted into their network testbed. Again, the job of the detection system is to find the attack sessions in the midst of normal background activity. Some systems may be tested in off-line mode, some in real-time mode, and some in both modes.

Schedule

Data for this first evaluation will be made available during the fall of 1998. The evaluation itself will occur in October and November. A follow-up meeting for evaluation participants and other interested parties will be held in December to discuss research findings. All R&D sites that find the task and the evaluation of interest are invited to participate.

For more information or to request copies of the training corpus, contact:

Dr. Marc A. Zissman or
Dr. Richard P. Lippmann
Lincoln Laboratory
Massachusetts Institute of Technology, Information Systems Technology Group
244 Wood Street
Lexington, MA 02420-9185
Voice: 781.981.7625
Fax: 781.981.0186
Email: INTRUSION@SST.LL.MIT.EDU
HTTP://WWW.LL.MIT.EDU/IST/

For specific information on the real-time evaluation, contact:

Terrence (Terry) G. Champion Air Force Research Laboratory
Electromagnetics Technology Division , INFOSEC Technology Office, Building 1124
Hanscom AFB, MA 01731-5000
Voice: 781.377.2068
Fax: 781.377.2563
Email: TGC@SAPPHO.RL.AF.MIL

Marc A. Zissman received the S.B. degree in computer science from MIT in 1985, and the S.B., S.M., and Ph.D. degrees in electrical engineering all from MIT in 1986, 1986, and 1990, respectively. He is presently assistant leader of the Information Systems Technology Group at MIT Lincoln Laboratory, where his research focuses on digital speech processing and computer network security. He may be reached at MAZ@SST.LL.MIT.EDU.

Richard P. Lippmann received a B.S. in electrical engineering from the Polytechnic Institute of Brooklyn in 1970 and a Ph.D. in electrical engineering from the Massachusetts Institute of Technology in 1978. He is presently a senior staff member in the Information Systems Technology Group at MIT Lincoln Laboratory, where his research focuses on speech recognition and the application of neural networks and statistics to problems in computer intrusion detection. He may be reached at RPL@SST.LL.MIT.EDU.

Defense Wide

continued from page 2

them, these two teams accomplish the overall mission, tasks, and functions of the DIAP and are staffed by a combination of Service, Joint Staff, OSD, and Defense Agency personnel. The FEIT consists of eight functional areas, including Readiness Assessment, Human Resources Development, Operational Policy and Doctrine Implementation, Security Management, Operational Monitoring, Architectural Standards and System Transformation, Acquisition and Product Development, and Research and Technology. These team members are the DIAP's principal evaluators for each functional area and will continuously evaluate Component IA programs to ensure the Defense-wide application of these functions is consistent, integrated, efficient, and programatically supported. The PDIT will provide for the oversight, coordination, and integration of the Department's IA resource programs. The sum total of these activities will ensure the Department's IA operational capabilities to protect, detect, and respond are appropriately met.

The transformation of IA from a largely technical issue to an operational imperative is critical to success of the Department's IA strategy. The DIAP constitutes a significant management, organizational, and cultural change within the Department. It will ensure that the Department's IA programs extend beyond traditional Service and Agency perspectives to meet the growing challenges of a dynamic, global information environment. Through this process, the Department will be able to leverage information and information technology to enhance the efficiency of its business activities and the impact of its military operations.

CAPT Burton received her M.S. in National Security Strategy from the National War College and her M.A. in Management Information Systems from George Washington University. She is currently assigned as the Staff Director, Defense-Wide Information Assurance Program (DIAP), in the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence.

The IATAC Information Assurance Tools Database hosts information on intrustion detection, vulnerability analysis, firewalls and antivirus applications. A brief summary of FIREWALL TOOLS is provided on these two pages. For more information, see the IATAC Product Order Form on page 15.

FIREWALLS

TITLE	COMPANY	KEYWORDS	URL
AltaVista Firewall 98	Digital Internet Solutions	Firewall, Application-Level Gateway, VPN	http://www.altavista.software.digital.com
AS/400	IBM, Inc.	Firewall, Application Gateway, Packet Filtering	http://www.ibm.com
Border Manager	Novell, Inc.	Firewall, Packet Filtering, Circuit-Level Gateways, Application-Level Gateways (Proxies), NAT, VPN	http://www.novell.com
BorderWare Firewall Server	BorderWare Technologies, Inc.	Firewall; Tri-Level: Packet Filtering, Circuit-Level Gateways, and Application Proxies; NAT, VPN	http://www.borderware.com
Brimstone/ Freestone	SOS Corporation	Firewall, Hybrid	http://www.soscorp.com
Checkpoint Firewall-1	Check Point	Firewall, Stateful Inspection, Proxies, NAT, VPN	http://www.checkpoint.com
clPro-FW	Radguard	Firewall, Multi-Layer Probing (MLP), NAT, VPN	http://www.radguard.com
ConSeal PC Firewall	Signal 9 Solutions	Firewall, Packet Filtering, NAT, VPN	http://www.signal9.com
CyberGuard for NT	CyberGuard Corporation	Firewall, Hybrid, NAT	http://www.cyberguard.com
CyberGuard for UnixWare	CyberGuard Corporation	Firewall, Hybrid, NAT	http://www.cyberguard.com
Elron Firewall	Elron Software, Inc.	Firewall, Stateful Inspection, NAT, VPN	http://www.elronsoftware.com
eNetwork for AIX/ Windows NT	IBM, Inc.	Firewall, Hybrid, NAT, VPN	http://www.ibm.com
Firebox 100/ Firebox II	WatchGuard Technologies, Inc	Firewall, Stateful Packet Filtering, Transparent Proxies, NAT, VPN	http://www.watchguard.com
Firewall for Windows NT	Secure Computing	Firewall, Application Gateway (Proxies)	http://www.elronsoftware.com
Gauntlet	Trusted Information Systems	Firewall, Application Gateway, VPN	http://www.tis.com
GemGuard	Gemini Computers	Firewall, Trusted Packet Filtering, VPN	http://www.geminisecure.com
GNAT Box	Global Technology	Firewall, Stateful Packet Inspection, Application Techniques, NAT	http://www.gnatbox.com
Guardian	NetGuard, Ltd.	Firewall, Stateful Inspection, NAT, VPN	http://www.ntguard.com
GuardIt	Computer Associates	Firewall, Hybrid, NAT	http://www.cai.com
He@tSeekerPro	Fortress Technologies	Firewall, Packet Filtering	http://www.fortresstech.com
ICE.BLOCK	J. River, Inc.	Firewall, Packet Filtering	http://www.jriver.com
Interceptor	Technologic, Inc.	Firewall, Application Proxies, VPN	http://www.tlogic.com

FIREWALLS

TITLE	COMPANY	KEYWORDS	URL
InterLock Service	WorldCom Advanced Networks	Firewall, Application-Level Proxy	http://www.ans.net
IOS Firewall Feature Set	Cisco Systems	Firewall, Packet Filtering, NAT, VPN	http://www.cisco.com
Lucent Managed Firewall	Lucent Technologies, Inc.	Firewall, Packet Filtering	http://www.lucent.com
LuciGate	Lucidata	Firewall, Packet Filtering, NAT	http://www.lucidata.com
NetGate	Small Works, Inc.	Firewall, Packet Filtering and Routing Package, VPN	http://www.smallworks.com
NetScreen-100/ NetScreen-10	NetScreen Technologies	Firewall, Dynamic Filter, NAT	http://www.netscreen.com
Norman Firewall	Norman Data Defense	Firewall, Dual-homed Gateway, Application Proxies, NAT	http://www.norman.com
PIX	Cisco Systems	Firewall, Hybrid, NAT	http://www.cisco.com
PORTUS-ES	Livermore Software Laboratories	Firewall, Proxies, NAT, VPN	http://www.lsli.com
PrivateWire	Cylink Corporation	Firewall, Dynamic Packet Filtering, VPN	http://www.cylink.com
PyroWall	Radguard	Firewall, Multi-Layer Probing (MLP), NAT, VPN	http://www.radguard.com
Raptor for NT	Axent Technologies	Firewall, Hybrid (Application-level proxies, Packet Filtering), NAT, VPN	http://www.axent.com
Raptor for Solaris	Axent Technologies	Firewall, Hybrid (Application-level proxies, Packet Filtering), NAT, VPN	http://www.axent.com
Secure Access	Ascend	Firewall, Hybrid, VPN	http://www.ascend.com
SecurIT Firewall for Solaris	Milkyway Networks	Firewall, Application and Circuit Level Gateway, Proxy Servers	http://www.milkyway.com
SecurIT Firewall for Windows NT	Milkyway Networks	Firewall, Application and Circuit Level Gateway, Proxy Servers	http://www.milkyway.com
SecureWare NetWall	Bull HN Information Systems	Firewall, Hybrid, NAT, VPN	http://www.bull.com
Sidewinder	Secure Computing	Firewall, Application Gateway (Proxies), VPN	http://www.securecomputing.com
SmartWall	V-ONE Corporation	Firewall, Packet Filtering, Proxies, NAT, VPN	http://www.v-one.com
Solstice Firewall-1	Sun Microsystems	Firewall, Stateful Inspection, VPN	http://www.sun.com/security
SonicWALL	Sonic Systems, Inc.	Firewall, Stateful Inspection, NAT	http://www.sonicsys.com
StoneBeat	Stonesoft Corporation	Firewall, High Availability	http://www.stonebeat.com
Telaxian Shield Firewall Server	Network Engineering	Firewall, Hybrid, NAT, VPN	http://www.fireants.com
WinGate	Deerfield Communications, Inc.	Firewall, Proxy server	http://www.deerfield.net

Detecting Intrusions Cooperatively Across Multiple Domains

by Donald L. Tobin, Jr.
University of Idaho

In the national defense arena, most analysts pay little attention to the isolated cases of computer intrusions reported almost weekly in the news. If analysts became aware of a pattern of attacks directed at a variety of networks and domains, however, this information might well warrant heightened attention. Our research efforts at the University of Idaho are directed in part at developing a prototype to supply multiple-domain information.

Commercial intrusion detection systems protect only a single network or a collection of networks in a single domain, such as pentagon.mil or lajes.af.mil. These limitations make it difficult even to detect a sweep or scan attack against multiple government and military installations in a single geographic area, especially if they represent different departments like the Department of Defense and the Department of Energy, or different services, such as the Army, Air Force, and Navy. A seemingly insignificant intrusion at one location would acquire much greater importance if collaboration among the installations revealed a coordinated set of attacks. Therefore, some form of data sharing is needed to detect systemic attacks against the nation's critical information infrastructure that involve multiple hosts and domains.

To help address these concerns, we have developed a prototype called HMMR (Hierarchical Management of Misuse Reports) or Hummer. The prototype and its source code are available at http://www.cs.uidaho.edu/~hummer. When HMMR is fully deployed, every host has a Hummer running on it, and all the hosts in a domain are probably, but not necessarily, arranged in some hierarchical fashion. Each domain has a top-level manager, and those managers may agree to form peer groups with top-level managers from other domains. Peer groups can also be formed among cooperating systems at other levels. In the hierarchical model, manager and subordinate systems do not have to be in the same domain.

The Hummers can collect data such as log files, usage reports, commercial tools, and freeware security tools and scanners from several locations on their host machine and put the acquired data into a common format. However, these capabilities require that additional coding to extract data from the source and then reformat it properly for the Hummer to use and distribute, depending on the filters created by that host's system administrator or high-level managers/administrators. The reformatted information is distributed, either through the hierarchy or to all the other peers in the peer group, The filter is simply a screen that determines which security-relevant information is to be shared with other hosts and networks. The filters can be generated quickly through one of the user interfaces.

Each Hummer has a World Wide Web-based interface for relatively easy configuration and management operations. The Audit Tool Manager lets the user pick which tools to use at any time. It also offers preconfigured suites of tools for "Possible Intrusion" and "Ongoing Intrusion" alert levels. These resources allow the operator to turn on all policy-defined tools and respond to a situation with only a few clicks of the mouse button. Once a top-level manager has created a particular configuration, he can push the configuration, including the filters to be used, out to all the other Hummers under him in the hierarchy in a few minutes.

The following scenario illustrates the Hummer's use. A Department of Energy (DOE) research laboratory located near an Army installation, an Air Force installation, and a major government contractor has formed a peer group with the other facilities using HMMR so the organizations may share security-related information. Normally, the data collection, logging, and auditing tools run in the background at the DOE lab; to avoid negative impact on the user community, only a small subset of Hummer tools are routinely turned on. One day, however, an alert system administrator sees Hummer-generated information being passed to her system from the Army installation and the government contractor, in turn, indicating they have been subjected to port scans. Expecting her network to be the next likely target, the system administrator turns on additional logging immediately, confident that with a few keystrokes, the more information she has, the better her chances of inhibiting the intruder.

Hummer represents only one of many areas in our ongoing research. The most important area, we believe, is developing a formal trust, integrity, and cooperation (TIC) model among hosts across multiple domains. We recognize that data, or even data requests, from a peer may be unreliable, inaccurate, or deliberately falsified, yet there remains a need to use available global information to ac-

continued on page 13

Secure Your Distributed Network: What Will It Take?

by Robert Duchatellier
Lucent Technologies

Today's enterprises rely on the World Wide Web to deliver timely information to a broad base of users, branch offices, partners, and customers. As more information, content, and applications become readily available via the Internet and via intranets and extranets, you must look closely at the security requirements of your organization's servers, systems, and networks and ensure that you protect these critical assets.

Intranets, extranets, and the Internet are changing our world. They distribute information and services to people, no matter where they are. But most network security systems were never designed for distributed environments. As a result, they cannot deliver the scalability and management control needed to support growth and still remain secure.

Web site databases and other application systems are compromised almost every day, sometimes inadvertently, sometimes with malicious intent, and sometimes for the so-called fun of "breaking in." No system is absolutely impervious to attack, from both internal and external individuals and groups, but you can take steps to protect your systems, and you can implement policies and procedures to reduce significantly the threat of unauthorized access. One approach to achieving these goals is use of the Lucent Managed Firewall, now available in version 3.0.

Originally engineered by Bell Labs to protect Lucent Technologies' networks, the Firewall is designed to be intrinsically secure. It physically separates the security and management functions to improve each function's security and performance.

Lucent Technologies

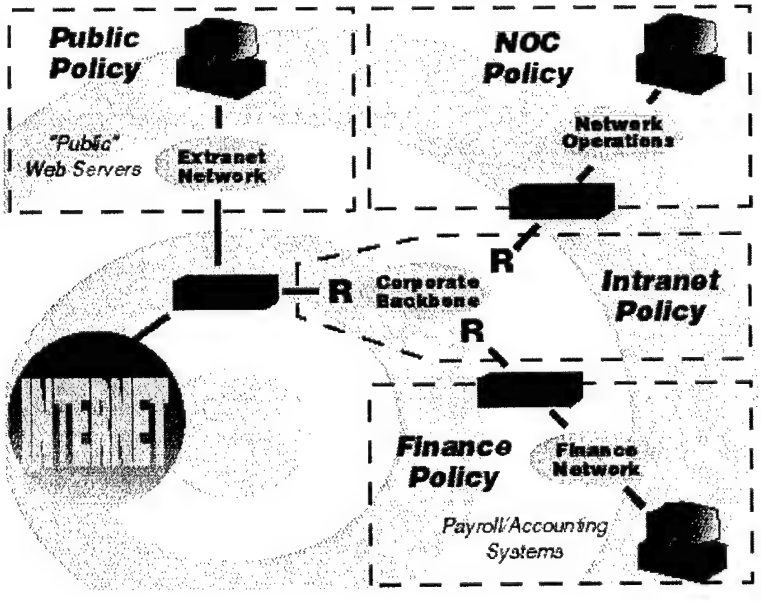
The Lucent network security appliance, called "the Brick," is a bridge-level device that runs Inferno™ operating system software, a compact, real-time operating system. The firewall code is embedded in the Inferno operating system kernel. The Brick eliminates common points of vulnerability, including user logins, files, hard drive, and monitor. The resulting firewall is hard to break and easy to maintain.

The Security Management Server software handles administrative functions. Available for Windows NT® and Sun Solaris® operating systems, the Security Management Server features an easy to use graphical user interface (GUI). As a result, network administrators do not have to be versed in operating systems or network configuration to manage the system.

The Brick uses native encryption and authentication features to communicate securely with the Security Management Server. The administrator works with the Security Management Server using encrypted sessions via industry-standard Secure Sockets Layer (SSL) and Design Engineering Services (DES) encrypted links, all of which are built in. Included with the Lucent Managed Firewalls is a free X.509 digital certificate from VeriSign.

Additionally, the Lucent Managed Firewall is extremely scalable and easy to deploy. Most firewalls establish security rules geographically or physically. Instead, Lucent uses security zones to establish rules logically. One Brick can support multiple security policies or "zones," and each security zone can be set up to have its own distinct set of rules, with report logs and alarms customized for that zone. Multiple zones can be managed centrally from one Security Management Server. This approach makes it easy for you to enforce multiple security policies across multiple Bricks, regardless of where your firewalls are located.

The Lucent Managed Firewall can easily scale up to meet your needs, no matter how large they become. As the network grows, you simply add Bricks to the Security Management System. Because the firewall appliance is implemented as a bridge, not a router, you can add new firewall appli-



continued on page 12

IA Scientific & Technical Information

by Robert P. Thompson
Director, IATAC

Collection of scientific and technical information (STI) is essential to Information Analysis Center (IAC) operations. The Information Assurance Technology Analysis Center (IATAC) collection of Information Assurance (IA) STI focuses on technologies that support the design, development, testing, evaluation, operations, and maintenance of Department of Defense (DoD) military systems and infrastructure. STI products and services serve to advance the knowledge base and productivity of the DoD research, development, test, and evaluation (RDT&E) community.

IATAC taps many sources to collect IA STI. It relies on direct interface with vendors supporting the IA community as a primary source of information. Nondisclosure agreements with corporations yield information on emerging research and development (R&D). Release of STI obtained through non-disclosure is tightly controlled as delineated in the agreement. Technical symposia and conferences also provide information, and seeks conference proceedings and technical papers often become part of the STI Collection. IATAC also interfaces with DoD and other Federal Government agencies also facilitate receipt of new scientific and technical information. Technical Area Tasks also produce's STI and helps to build the IA collection. Finally, open source gathering techniques augment collection activities. The IATAC collection offers matierials on a number of IA STI topics, including those listed below.

Information in the IA STI collection is available to registered Defense Technical Information Center (DTIC) users. Secondary distribution instructions must be strictly followed to ensure compliance with copyright restrictions. To become a registered DTIC user, applicants must complete DD Form 1540 available from http://web1.whs.osd.mil/icdhome/DDEFORMS.HTM.

For more information on the IA STI Collection, contact IATAC at 703.902.3177 or via email at iatac@dtic.mil.

STI Topics

- Command, Control, Communications, Computers & Intelligence (C4I)
- Computer Network Attacks (CNA)
- Encryption
- Firewalls
- Hackers
- Information Assurance
- Information Operations
- Information Warfare
- Infrastructure Assurance
- Intrusion Detection
- Malicious Code Detection
- Red Teaming
- Vulnerability Analysis
- Virus/Anti-Virus
- Year 2000 (Y2K)

Secure Your Network

continued from page 11

ances at any time without reconfiguring the router network. With the release of the Lucent Managed Firewall v3.0, you can also manage software downloads remotely, saving time and maintenance expense.

The Lucent Managed Firewall can operate in a gateway perimeter setting to protect an enterprise network from the Internet or from partner extranet networks. It can separate public Web servers from sensitive intranet servers. It can also separate different intranet segments. Its scalability and flexibility can handle virtually any type of appliction, as well as any size and type of infrastructure.

Your network applications and systems are only as secure as the weakest point of entry. To secure your network, you must design the system to provide distributed security, centralized management and scalability. You must also adhere to strict policies and train users effectively. Implementing these steps and deploying advanced firewall technology will provide a secure system to support a broad range of applications, while minimizing the threat from unwelcome guests. These components build the strong foundation required to ensure maximum security while they also deliver the flexibility needed to grow your enterprise.

For more information, contact Lucent Technologies at 888.552.2544 or on-line at http://www.lucent.com/security.

Robert Duchatellier received an M.S. in Indusrial and Applied Mathematics from Brooklyn Polytechnics Institute and an M.S. in Technology Management from Stevens Institute of Technology. He is currenlty Lucent Technologies' Lucent Managed Firewall Sales Channel Manager for the U.S. Government, Department of Defense, and Federal Agencies.

NOV 1-5

25th Annual Computer Security Conference & Exhibition
Sponsored by Computer Security Institute (CSI)
Chicago, IL
call 415.905.2378
www.gocsi.com

NOV 2-5

The Defense Technical Infor mation Center (DTIC) Annual Users Meeting and Training Confer ence
DoubleTree Hotel
National Airport, Arlington, VA
call Ms. Julia Foscue
703.767.8236
jfoscue@dtic.mil
http://www.dtic.mil

NOV 4-5

13th Annual Mid-Atlantic Intelligence Symposium
Sponsored by AFCEA Central Maryland Chapter
Johns Hopkins Applied Physical Lab (APL), Laurel, MD
call Dawn Metzer 410.684.6580

JAN 19-21

AFCEA West '99
Sponsored by AFCEA and the U.S. Naval Institute
San Diego, CA
call the AFCEA Programs Office
703.631.6125 / 6126

MAR 2-4

Southeast C4I Conference and Exposition
Sponsored by the AFCEA Tampa — St. Petersburg Chapter
Tampa, FL
call J. Spargo & Associates
703.631.6200

DTIC's Annual Users Meeting & Training Conference

This year DTIC is hosting its 25th Annual Users Meeting and Training Conference. The conference will be held at the DoubleTree Hotel National Airport, 300 Army Navy Drive, Arlington, VA, from 2-5 November 1998. The agenda is packed full of exciting and relevant topics, as well as an exhibit room overflowing with vendors from every aspect of Information Technology (IT).

"Maintaining the Information Edge" is the theme for the conference, and the sessions are geared to this topic. DTIC '98 will address the information sources and changing technologies that impact those who are involved in Defense Research and Acquisition. We are particularly pleased to announce this year's keynote speakers: Lieutenant General David J. Kelley, Director, Defense Information Systems Agency; Mr. Carol Cini, Associate Director, U.S. Government Printing Office; and Mr. Richard Luce, Director, Los Alamos Research Library. Mr. Louis Purnell, the luncheon speaker, will be relating his exploits during World War II as a Tuskeegee Airman.

The Conference offers four days of varied training sessions that enable DTIC users to collaborate on the latest IT topics. Presentations will address the most current issues effecting the research, development, and acquisition communities. Not only will these speakers acquaint you with the latest policy and operational developments, but they will also provide you with practical details on valuable and diverse domestic and foreign information resources, security issues, the World Wide Web, virtual libraries, video streaming and the storage and dissemination of electronic documents.

Maintaining the Information Edge presents exciting new challenges — DTIC '98 promises to provide the tools to expand your horizons to meet these challenges! For more information, please contact Ms. Julia Foscue, the DTIC '98 Conference Coordinator at 703.767.8236 or via e-mail: jfoscue@dtic.mil, or access the DTIC homepage at http://www.dtic.mil.

Detecting Intrusions

continued from page 10

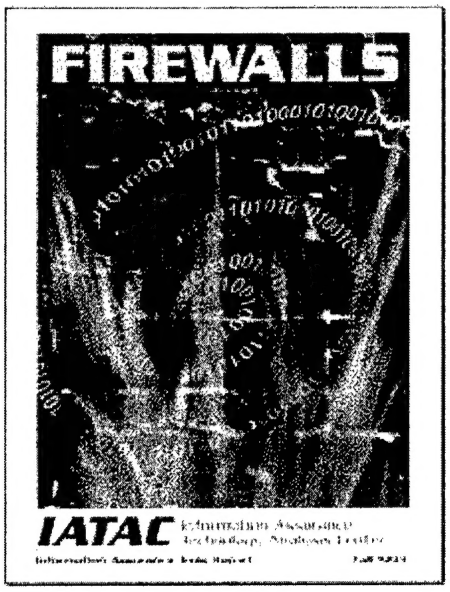
curately assess the local security posture. Therefore, a formal model must include multiple levels of cooperation and trust and must provide concise definitions of cooperation and trust in this context. Other considerations to be addressed are whether the cooperation levels should be statically or dynamically assigned and how quickly or gracefully they should be adjusted in response to the most current data. The model must also take into account the various costs of cooperation, including data collection, transmission, and sanitization and the exposure risk of the local network.

While most of the structure has been coded by undergraduates (Jamie Marconi, Jesse McConnell, Dean Polla, and Joel Marlow) so far, we hope our work on Project HMMR and our future research will encourage other researchers to explore new ideas for addressing the risks facing the critical information infrastructure. We have shown that cooperative intrusion detection can be achieved, and we believe it must be achieved to help ensure national security in the future.

Donald Tobin. is a doctoral student at the University of Idaho and a research assistant at the Center for Secure and Dependable Software. His primary research interests are in intrusion detection, neural networks, and information warfare. He is a retired Air Force officer and has worked with a variety of communication, satellite, and missile warning systems. He earned his M.S. in Computer Science from Boston University and his B.S. in Mathematics from the University of Texas.

IA Tools Report: FIREWALLS

New Products



The Information Assurance (IA) Tools Report on Firewall tools is now available to registered DTIC users. This report provides an index of firewall products contained in the IA Tools database. It summarizes pertinent information, providing users with a brief description of available tools and contact information. As a living document, this report will be updated periodically as additional information is entered into the database.

Currently the IA tools database contains 46 firewall tools that are available in the commercial marketplace or through GSA contracts. The firewall products provide a range of solutions to meet various firewall requirements. These solutions can provide protection of internal networks and provide secure Internet and remote access connections. The database was built by gathering open-source data, analyzing that data, coordinating with the respective firewall developer, and then formatting the data into the final report. The information includes a basic description, security services and mechanisms, availability, contact, and reseller/ distributors for each firewall product included. For instructions on obtaining a copy of this report, refer to the IATAC Product Order Form.

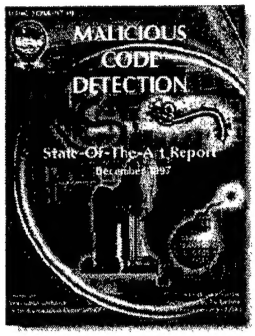
IA Tools Reports — Vulnerability Analysis & Intrusion Detection

This IA Tools reports summarize pertinent information, providing users with a brief description of available tools and contact information. As living documents, these reports will be updated periodically as additional information is entered into the databases.

Currently the Vulnerability Analysis IA Tools database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment. Research for the Intrusion Detection IA Tools report identified 43 intrusion detection tools currently employed and available.

Modeling & Simulation Technical Report

This report describes the models, simulations and tools being used or developed by selected organizations that are chartered with the IA mission. The definitions prescribed by DMSO for model and simulation were used to determine what entities should be included in this IA models, simulations and tools report.



Malicious Code Detection State-Of-The-Art Report

This SOAR addresses malicious software detection. Included is a taxonomy for malicious software to provide the audience with a better understanding of commercial malicious software. An overview of the current state-of-the-art commercial products and initiatives, as well as future trends is presented. The same is then done for current state-of-the-art in regards to DoD. Lastly, the report presents observations and assertions to support the DoD as it grapples with this problem entering the 21st century.

IATAC Product Order Form

IMPORTANT NOTE: *All IATAC Products are distributed through the Defense Technical Information Center (DTIC). If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. To register with DTIC go to http://www.dtic.mil/dtic/regprocess.html.*

Name _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

_____

DoD Organization? ❑ YES ❑ NO If NO, complete **LIMITED DISTRIBUTION** section below.

LIMITED DISTRIBUTION	QTY.	PRICE EA.	EXTD. PRICE
In order for NON-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218			
Contract No. _____ *For contractors to obtain reports, request must support a program & be verified with COTR*			
COTR _____ Phone _____			
❑ **Modeling & Simulation Technical Report**		No Cost	
❑ **IA Tools Report — Firewalls**		No Cost	
❑ **IA Tools Report — Intrusion Detection**		No Cost	
❑ **IA Tools Report — Vulnerability Analysis**		No Cost	
❑ **Malicious Code Detection SOAR** ❑ TOP SECRET ❑ SECRET		No Cost	

Security POC _____ Security Phone _____

UNLIMITED DISTRIBUTION	QTY.	PRICE EA.	EXTD. PRICE
❑ **Newsletters** *(Limited number of back issues available)*			
❑ Vol. 1, No. 1 ❑ Vol. 1 No. 2 ❑ Vol. 1 No. 3 ❑ Vol. 2, No. 1 ❑ Vol. 2 No. 2		No Cost	
		ORDER TOTAL	

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: _____

_____

_____

Once completed, Fax to IATAC at 703.902.3425

ARE sharing your IA newsletter

For Additions, Deletions and Changes

— U.S. Distribution Only —
Copy this page, complete the form and fax to IATAC at 703.902.3425

❑ Change ❑ Add ❑ Delete

Name_____ Title _____

Company/Org._____

Address _____

_____

City/State_____ Zip_____

Phone _____ Fax _____

DSN_____ E-mail _____

Organization (check one):

❑ USA ❑ USN ❑ USAF ❑ USMC ❑ OSD ❑ Contractor ❑ Other_____

Information Assurance
Technology Analysis Center
8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838